



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/357,726	07/21/1999	DAVID L. WOOD	1004-3633	9654

42714 7590 04/05/2006

ZAGORIN O'BRIEN GRAHAM LLP (004)
7600B NORTH CAPITAL OF TEXAS HIGHWAY
SUITE 350
AUSTIN, TX 78731-1191

EXAMINER

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/357,726	WOOD ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 10-12, 17-26, 30-35 and 38-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 10-12, 17-26, 30-35 and 38-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 July 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the arguments filed on 30 December 2005.
2. Claims 10-12, 17-26, 30-35 and 38-41 are pending in the application.
3. Claims 10-12, 17-26, 30-35 and 38-41 have been rejected.
4. Claims 1-9, 13-16, 27-29, 36 and 37 have been cancelled.

Response to Arguments

6. Applicant's arguments with respect to claims 17-26, 30-35 and 38-41 have been considered but are moot in view of the new ground(s) of rejection.
7. The indicated allowability of claims 10-12, 17-26, 30-35 and 38-41 is withdrawn in view of the newly discovered reference(s) to Robins et al. Rejections based on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. **Claims 10-12, 17-26, 30-35 and 38-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Robins et al U.S. Patent No. 6,115,744.**

As to claim 10, Robins et al discloses a method of securing a data transaction across a security barrier, the method comprising:

validating a request message encoded in a structured request language against a predefined request message specification therefor [column 7 line 36 to column 9 line 48];

transmitting the validated request message across the security barrier [column 7 line 36 to column 9 line 48];

validating a response message encoded in a structured response language against a predefined response message specification thereof, the response message corresponding to the validated request [column 9 line 51 to column 10 line 64];
and

transmitting the validated response message across the security barrier [column 9 line 51 to column 10 line 64],

wherein the request and the response message validatings are respectively performed at first and second secure brokers on opposing sides of the security barrier [column 7 line 36 to column 9 line 48]; and

wherein the validated request and response message transmissions are between the first and second secure data brokers [column 7 line 36 to column 9 line 48].

As to claim 11, Robins et al discloses a method of securing a data transaction across a security barrier, the method comprising:

validating a request message encoded in a structured request language against a predefined request message specification thereof [column 7 line 36 to column 9 line 48];

transmitting the validated request message across the security barrier [column 7 line 36 to column 9 line 48];

validating a response message encoded in a structured response language against a predefined response message specification thereof, the response message corresponding to the validated request [column 9 line 51 to column 10 line 64];
and

transmitting the validated response message across the security barrier [column 7 line 36 to column 9 line 48],

wherein the request message validating includes:

parsing the request message using Data Type Definitions (DTDs) encoding a hierarch of valid tag-value pairs in accordance with syntax of a valid request message [column 7 line 36 to column 9 line 48]; and

if the request message is not successfully parsed, forwarding a response message without transmission of the request message across the security barrier [column 7 line 36 to column 9 line 48].

As to claim 12, Robins et al discloses a method of securing a data transaction across a security barrier, the method comprising:

- validating a request message encoded in a structured request language against a predefined request message specification therefor [column 7 line 36 to column 9 line 48];

- transmitting the validated request message across the security barrier [column 7 line 36 to column 9 line 48];

- validating a response message encoded in a structured response language against a predefined response message specification therefor, the response message corresponding to the validated request [column 9 line 51 to column 10 line 64]; and

- transmitting the validated response message across the security barrier [column 9 line 51 to column 10 line 64],

- wherein the response message validating includes:

- parsing the response message using Data Type Definitions (DTDs) encoding a hierarchy of tag-value pairs in accordance with syntax of a valid response message [column 9 line 51 to column 10 line 64].

As to claim 17, Robins et al discloses in a networked computing environment, a method of securing access to an information resource behind a security barrier, the method comprising:

- predefining a request message specification corresponding to a structured request language [column 7 line 36 to column 9 line 48];

formatting an access request in accordance in accordance with the structured request language [column 7 line 36 to column 9 line 48];

supplying the formatted access request to a first intermediary [column 7 line 36 to column 9 line 48], the intermediary validating the formatted access request in accordance with the request message specification [column 7 line 36 to column 9 line 48]; and

forwarding the validated access request across the security barrier [column 7 line 36 to column 9 line 48].

As to claim 18, Robins et al discloses a method further comprising:

accessing the information resource in accordance with the validated request [column 10 line 66 to column 12 line 46].

As to claim 19, Robins discloses a method further comprising:

receiving, at an application proxy, an access request targeting the information resource [column 10 line 66 to column 12 line 46]; and

performing the access request formatting at the application proxy [column 10 line 66 to column 12 line 46].

As to claim 20, Robins discloses a method further comprising:

predefining a response message specification corresponding to a structured response language [column 9 line 51 to column 10 line 64];

formatting a response to the access request in accordance with the structured language [column 9 line 51 to column 10 line 64];

supplying the formatted response to a second intermediary, the second intermediary validating the formatted response in accordance with the response message specification [column 9 line 51 to column 10 line 64]; and

forwarding a validated response across the security barrier [column 9 line 51 to column 10 line 64].

As to claim 21, Robins et al discloses a method further comprising:

accessing the information resource in accordance with an access request from a client [column 7 line 36 to column 9 line 48]; and

supplying the client with a response in accordance with the validated response [column 7 line 36 to column 9 line 48].

As to claim 22, Robins et al discloses in a networked computing environment, a method of securing access to an information resource behind a security barrier, the method comprising:

predefining a response message specification corresponding to a structured response language [column 9 line 51 to column 10 line 64];

formatting a response to an access request targeting the information resource, the formatted response being in accordance with the structured response language [column 9 line 51 to column 10 line 64];

supplying the formatted response to an intermediary, the intermediary validating the formatted response in accordance with the response message specification [column 9 line 51 to column 10 line 64]; and

forwarding a validated response across the security barrier [column 9 line 51 to column 10 line 64].

As to claim 23, Robins et al discloses a method further comprising:

accessing the information resource in accordance with the access request from a client [column 10 line 66 to column 12 line 46];

supplying the client with a response in accordance with the validated response [column 10 line 66 to column 12 line 46].

As to claim 24, Robins et al discloses an information security system comprising;

a security barrier [column 7 line 36 to column 9 line 48];

a proxy for an information resource, the proxy and the information resource on opposing first and second sides, respectively, of the security barrier [column 7 line 36 to column 9 line 48];

a data broker on the first side of the security barrier, wherein, in response to an access request targeting the information resource, the data broker validates a request message encoded in a structured request language against a predefined request message specification therefor and forwards only validated request messages across the security barrier [column 7 line 36 to column 9 line 48].

As to claim 25, Robins et al discloses an information security system further comprising:

a second data broker on the second side of the security barrier, wherein, in response to an access targeting the information resource, the second data broker validates a response message against a predefined response message specification and forwards only validated response messages across the security barrier [column 9 line 51 to column 10 line 64].

As to claim 26, Robins et al discloses an information security system further comprising:

the information resource [column 10 line 66 to column 12 line 46].

As to claim 30, Robins et al discloses a computer program product encoded in computer readable media, the computer product comprising:

data broker code and parser code executable on a first network server separated from an information resource by a security barrier [column 7 line 36 to column 9 line 48];

the data broker code including instructions executable as a first instance thereof to receive access requests in a structured language corresponding to a predefined request message specification and to forward validated ones of the access requests across the security barrier toward the information resource [column 7 line 36 to column 9 line 48]; and

the parser code including instructions executable as a first instance thereof to validate the received access requests against the predefined request message specification [column 7 line 36 to column 9 line 48].

As to claim 31, Robins et al discloses the computer program product further comprising:

an encoding of the predefined request message specification [column 7 line 36 to column 9 line 48].

As to claim 32, Robins et al discloses the computer program product,

wherein the data broker code and parser code are also executable on a second network server separated from a client application by the security barrier [column 9 line 51 to column 10 line 64];

wherein the data broker code includes instructions executable as a second instance thereof to receive responses in a structured language corresponding to a predefined response message specification and to forward validated ones of the responses across the security barrier toward the client application [column 9 line 51 to column 10 line 64]; and

wherein the parser code includes instructions executable as a second instance thereof to validate the received responses against the predefined response message specification [column 9 line 51 to column 10 line 64].

As to claim 33, Robins et al discloses the computer program product further comprising:

an encoding of the predefined response message specification [column 9 line 51 to column 10 line 64].

As to claim 34, Robins et al discloses the computer program product further comprising:

application proxy code including instructions executable to format the access request in accordance with the structured language corresponding to the predefined request message specification [column 7 line 36 to column 9 line 64].

As to claim 35, Robins et al discloses the computer program product encoded by or transmitted in at least one computer readable medium selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium [column 10 line 66 to column 12 line 46].

As to claims 38-41, Robins et al discloses that the markup language includes extensible markup language [column 9, lines 31-48].

Art Unit: 2131

Conclusion


9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
March 28, 2006




AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100